Listing of Claims

1. (Original) A system for providing public key cryptography including assistance in recovery of messages sent to users, the method comprising:

a first key pair generated for a particular user, the first key pair comprising a public key employed for encrypting messages sent to the particular user and comprising a private key employed for decrypting messages which have been encrypted using the public key of the first key pair;

a second key pair generated for message recovery, the second key pair comprising a public key employed for recovering messages which have been encrypted using the public key of the first key pair and comprising a private key employed for decrypting messages which have been encrypted using the public key of the second key pair;

information referencing the public key of the second key pair embedded within the public key of the first key pair; and

an encryption module automatically employing the public key of the second key pair during encryption of the message under the public key of the first key pair so that the message being encrypted can be directly decrypted using the private key of the second key pair.

2. (Original) A system according to Claim 1, further comprising:

information which uniquely identifies the public key of the second key pair stored into the public key of the first key pair.

3. (Original) A system according to Claim 2, wherein said information which uniquely identifies the public key of the second key pair includes information pointing to a location where the second key pair is stored.

4. (Original) A system according to Claim 1, further comprising:

a copy of the public key of the second key pair embedded within the public key of the first key pair.

5. (Original) A system according to Claim 1, further comprising:

assertion information appended to the public key of the first key pair, said assertion information including a pointer which uniquely identifies the public key of the second key pair.

6. (Original) A system according to Claim 5, wherein said assertion information includes constraints specifying use of the public key of the first key pair.

7. (Original) A system according to Claim 6, wherein the constraints include a constraint specifying that use of the public key of the second key pair is mandatory during encryption of a message using the public key of the first key pair.

8. (Original) A system according to Claim 1, wherein at least one key pair comprises a Diffie-Hellman-compatible key pair.

9. (Original) A system according to Claim 1, wherein at least one key pair comprises an RSA-compatible key pair.

10. (Original) A system according to Claim 1, wherein said message being encrypted comprises a selected one of a text file and a binary file.

11. (Original) In a computer system providing public key cryptography, a method for assisting with recovery of messages sent to users, the method comprising:

generating a first key pair for a particular user, the first key pair comprising a public key employed for encrypting messages sent to the particular user and comprising a private key employed for decrypting messages which have been encrypted using the public key of the first key pair;

generating a second key pair for message recovery, the second key pair comprising a public key employed for recovering messages which have been encrypted using the public key of the first key pair and comprising a private key employed for decrypting messages which have been encrypted using the public key of the second key pair;

embedding within the public key of the first key pair information referencing the public key of the second key pair; and

automatically employing the public key of the second key pair during encryption of the message under the public key of the first key pair so that the message being encrypted can be directly decrypted using the private key of the second key pair.

12. (Original) A method according to Claim 11, further comprising:
storing information which uniquely identifies the public key of the second key pair.

13. (Original) A method according to Claim 12, wherein said information which uniquely identifies the public key of the second key pair includes information pointing to a location where the second key pair is stored.

14. (Original) A method according to Claim 11, further comprising:
storing a copy of the public key of the second key pair embedded within the public key of the first key pair.

15. (Original) A method according to Claim 11, further comprising:
appending assertion information to the public key of the first key pair, said assertion information including a pointer which uniquely identifies the public key of the second key pair.

16. (Original) A method according to Claim 15, wherein said assertion information includes constraints specifying use of the public key of the first key pair.

17. (Original) A method according to Claim 16, wherein the constraints include a constraint specifying that use of the public key of the second key pair is mandatory during encryption of a message using the public key of the first key pair.

18. (Original) A method according to Claim 11, wherein at least one key pair comprises a Diffie-Hellman-compatible key pair.

19. (Original) A method according to Claim 11, wherein at least one key pair comprises an RSA-compatible key pair.

20. (Original) A method according to Claim 11, wherein said message being encrypted comprises a selected one of a text file and a binary file.

21. (Currently Amended) A computer-readable storage medium ~~holding code~~ having computer executable instructions for performing the method according to Claims 11, 12, 14 ~~and~~ or 15.

22. (Previously Presented) A public key encryption system integrating a message recovery key, comprising:

a session encryption module block-cipher encrypting a plaintext message into cyphertext using a session key;

a public key encryption module encrypting the session key using a public key of a user, the public key of the user being associated with a private key generated simultaneously thereto and encrypting the session key using a public key of a message recovery agent automatically triggered upon use of the public key of the user, the public key of the message recovery agent being associated with a private key generated simultaneously thereto;

a digital envelope forming an encrypted message comprising the cyphertext and the encrypted session key;

a reference stored into the public key of the user to automatically use the public key of the message recovery agent upon use of the public key of the user;

a pointer to the public key of the message recovery agent embedded as the reference into the public key of the user; and

at least one of a cryptographic hash and a message digest of the pointer stored as the reference to the public key of the message recovery agent.

23. (Original) A system according to Claim 22, further comprising:

a public key decryption module decrypting the encrypted message by the user, by decrypting the encrypted session key using the private key of the user and block-cipher decrypting the cyphertext using the decrypted session key.

24. (Original) A system according to Claim 22, further comprising:

a public key decryption module decrypting the encrypted message by the message recovery agent, by decrypting the encrypted session key using the private key of the message recovery agent and block-cipher decrypting the cyphertext using the decrypted session key.

25. (Cancelled).

26. (Previously Presented) A system according to Claim 22, further comprising:

the public key of the message recovery agent embedded as the reference into the public key of the user.

27. (Cancelled).

28. (Cancelled).

29. (Previously Presented) A system according to Claim 22, further comprising:

a digital signature formed from the private key of the user; and

the reference stored into the public key of the user upon successfully authenticating the digital signature.

30. (Previously Presented) A method for integrating a message recovery key into a public key encryption system, comprising:

block-cipher encrypting a plaintext message into cyphertext using a session key;

encrypting the session key using a public key of a user, the public key of the user being associated with a private key generated simultaneously thereto;

encrypting the session key using a public key of a message recovery agent automatically triggered upon use of the public key of the user, the public key of the message recovery agent being associated with a private key generated simultaneously thereto;

forming an encrypted message comprising the cyphertext and the encrypted session key;

providing a reference into the public key of the user to automatically use the public key of the message recovery agent upon use of the public key of the user;

embedding a pointer to the public key of the message recovery agent as the reference into the public key of the user; and

storing the reference as at least one of a cryptographic hash and a message digest of the pointer to the public key of the message recovery agent.

31. (Original) A method according to Claim 30, further comprising:

decrypting the encrypted message by the user, comprising:

decrypting the encrypted session key using the private key of the user; and

block-cipher decrypting the cyphertext using the decrypted session key.

32. (Original) A method according to Claim 30, further comprising:

decrypting the encrypted message by the message recovery agent, comprising:

decrypting the encrypted session key using the private key of the message recovery agent; and

block-cipher decrypting the cyphertext using the decrypted session key.

33. (Cancelled).

34. (Previously Presented) A method according to Claim 30, further comprising:

embedding the public key of the message recovery agent as the reference into the public key of the user.

35. (Cancelled).

36. (Cancelled).

37. (Previously Presented) A method according to Claim 30, further comprising:

forming a digital signature from the private key of the user; and

storing the reference into the public key of the user upon successfully authenticating the digital signature.

38. (Currently Amended) A computer-readable storage medium ~~holding code~~ having computer executable instructions for performing the method according to Claims 30, 31, ~~and~~ or 32.

39. (Cancelled).

40. (Cancelled).

41. (Cancelled).

42. (Cancelled).

43. (Cancelled).